The title has been changed as requested, and Fig. 12 has been resubmitted with proper margins. In addition, the disclosure has been amended as required, and to correct various informalities. Withdrawal of the objections in paragraphs 1, 2 and 3 of the office action is respectfully requested.

Claims 7 and 14 stand rejected under § 112. Claims 7 and 14 have been amended to overcome this rejection, without narrowing the scope of the claims. Reconsideration and withdrawal are respectfully requested.

Claim 15 stands rejected under § 102 on the basis of Al-Salqan, and claims 1-6 stand rejected under § 103 on the basis of Al-Salqan and Dumas et al. or Schneier. Applicants respectfully traverse these rejections because none of the references, alone or in combination, disclose or suggest methods or apparatus in which key data that encrypts data is different for each unit storage area of the storage medium, as recited in the rejected claims as amended, and newly added claims 16-19.

Al-Salqan merely discloses a key data encryption and decoding method with a password for storage. Dumas et al. merely disclose a data encryption method with a single key for a hard disk drive, and Schneier merely discloses a random key generating method. None of the references disclose or suggest the present invention, in which the key data which encrypts the data is different for each unit storage area of the storage medium.

For the foregoing reasons, applicants believe that this case is in condition for allowance, which is respectfully requested. The examiner should call applicants' attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns
Registration No. 29,367

August 8, 2001

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Facsimile: 312.360.9315
F:\DATA\WP60\3408\62676\ame-a.doc

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Specification:

The paragraph beginning on page 2, line 5, was amended as follows:

There arise, however, [the] several problems inherent in the prior art.

The paragraph beginning on page 2, line 7 was amended as follows:

First, as cipher texts defined as samples or combinations of the cipher texts with unencrypted plain texts become larger in quantity, the decryption by a decipherer becomes easier. [A result into which] As a result, the same plain text is encrypted with the same password [, is equal]. Therefore, when encrypted directly with the same password, a statistic characteristic of the cipher text reflects in a statistic character of the plain text. Accordingly, a conventional method of encrypting with the same password on the storage medium presents such a problem that if a volume of the cipher texts is large enough to make a statistic process executable, the characteristics of the plain texts can be presumed easily.

The paragraph beginning on page 2, line 19 was amended as follows:

Second, data is stored in a large capacity storage medium such as an optical disk etc. [is stored with the data, of which some] A portion of the data such as a directory portion is structured in a fixed format. A problem peculiar to the conventional method of

encrypting with the same password on the storage medium is that the password is presumed by analyzing this portion, in which case other vital data are to be deciphered.

The paragraph beginning on page 2, line 26 was amended as follows:

Third, according to the conventional method of setting the password per file, when the password of some portion is decrypted, other portions can be prevented from being decrypted. In this case, however, it is required that [he] the different password be managed per file. This operation is troublesome and might cause a problem in which a fault such as forgetting the password and so on can easily [is easy to] occur.

The paragraph beginning on page 3, line 6 was amended as follows:

Fourth, in the large capacity exchangeable storage medium such as an optical disk etc, it is possible to [carry] take the storage medium out and copy the storage medium. Therefore, the once-encrypted data is carried out and may be analyzed later on taking a sufficient period of time. Accordingly, the problem is that the password is easy to be presumed form the cipher text.

The paragraph beginning on page 3, line 12 was amended as follows:

A fifth[,] problem is that the data has hitherto been encrypted directly with the password, and hence, if the password is changed, the whole data are required to be re-encrypted.

The paragraph beginning on page 3, line 17 was amended as follows:

It is a primary object of the present invention to provide a method of and an apparatus for protecting data on a storage medium, wherein a password is not easily discovered [hard to be analyzed] from a cipher text.

The paragraph beginning on page 4, line 13 was amended as follows::

According to the present invention, the data is encrypted not by using the password directly as an encryption key but by using key data generated separately. The key data is encrypted with the password serving as a key, and written to the storage medium. When in the reading process, the encrypted key data is decoded with the password, thereby obtaining the key data. Then, the data is decoded with the key data.

The paragraph beginning on page 4, line 20 was amended as follows:

Thus, the data is encrypted by use of the key data generated separately from the password, whereby the encrypted key data is, even if a cipher text is to be analyzed, merely decrypted. The password and the key data are therefore hard to analyze [be analyzed]. This makes it feasible to prevent the password from being deciphered by analyzing the cipher text.

The paragraph beginning on page 8, line 21 was amended as follows:

As illustrated in FIG. 4, the logical format of the storage medium (disk) 1 is shown by each sector. This sector is addressed based on a logical block address LBA. Herein, in FIG. 4, there are provided X-pieces of sectors of logical block addresses LBA being [1] through [X].

The paragraph beginning on page 8, line 26 was amended as follows:

The region L1 for a [-] sector starting from a head sector (LBA = 1) within the storage area of the optical disk, is allocated as a storage region for the encrypted key data PS′ [1] - PS′ [n]. [.] namely, the number of sectors in a use [using] region of the data is n (= (X-a)), and, per section in the use [using] region, the encrypted key data PS′ [1] - PS′ [n] are stored in the region L1.

The paragraph beginning on page 15, line 8 was amended as follows:

When in a medium logical formatting process, as in the first embodiment shown in FIG. 2, the region L1 on the optical disk 1 is stored with encrypted key data PS′ [1] - PS′ [512]. Herein, however, the encrypted data is not stored per logic sector. For example, it is assumed that a capacity of the region L1 be 4 KB. Then, supposing that the password [be] is an 8-byte/entry, as shown in FIG. 9, 512-pieces of key words (entries) PS[1] - PS [512] are generated. Subsequently, the region L1 is stored with the 512-pieces of encrypted key words PS′ [1] - PS′ [512].

The paragraph beginning on page 18, line 25 was amended as follows:

The size of the region L on the optical disk 1 can be made smaller in the third embodiment than in the first embodiment. Namely, it is required in the first embodiment that the same number of pieces of key data as the number of the logic sectors be stored. For instance, supposing that one sector [be] is 2 KB, the storage capacity be 600 MB and the key data by 8 bytes, the region L1 is required to have a capacity of 2.4 MB. In the third embodiment, 512-pieces of key data are stored, and therefore approximately 4 KB may suffice for the region L1.

The paragraph beginning on page 21, line 9 was amended as follows:

(S62) The CPU 2, if the data in the region L1 have not been read out, executes the process of developing the key data in the operation region of the memory 3. Namely, the CPU 2 obtains the user password Pwi. Then, the CPU 2 reads the data from a region Li and decodes the read data with the password Pwi. The password PW1 is thereby obtained[.] on the optical disk 1.

In the Claims:

New claims 16-19 were added and claims 1, 3, 7, 8, 10, 14 and 15 were amended as follows:

1. (Amended) A storage medium data protecting method of protecting data on a storage medium, comprising:

a step of generating key data, encrypting the key data with a password, and writing the encrypted key data to said storage medium;

a step of encrypting the data with the key data, and writing the encrypted data to said storage medium;

a step of reading the encrypted key data from said storage medium;

a step of decoding the encrypted key data with the password; and

a step of decoding the data on said storage medium with the decoded key data[.],

wherein said key data generating step comprises a step of generating different key data for each of a plurality of unit storage areas of said storage medium.

3. (Amended) A storage medium data protecting method according to claim [2]1, wherein said key data generating step comprises a step of generating is [the] different key data [per logic sector on said storage medium when writing the data] for each writing to said unit storage areas.

7. (Amended) A storage medium data protecting method according to claim 1, wherein said step of writing the encrypted key data to said storage medium comprises a step of encrypting the key data with a first [one] password, writing the encrypted key data to said storage medium, encrypting a second

[other] password with said first [one] password, and writing said second [other] encrypted password, and

said step of decoding the key data comprises a step of decoding said second [other] encrypted password with said second [the other] password, and obtaining said first [the one] password, and a step of decoding the encrypted key data with said first [the one] password.

8. (Amended) A storage medium data protecting apparatus for protecting data on a storage medium, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating key data, the key data with a password, writing the encrypted key data to said storage medium, encrypting the data with the key data, and writing the encrypted data to said storage medium;

a read mode of encoding, after reading the encrypted key data from said storage medium, the encrypted key data with the password, and decoding the data on said storage medium with the decoded key data[.],

wherein said key data comprises different key data for each unit storage area of said storage medium.

10. (Amended) A storage medium data protecting apparatus according to claim [9] 8, wherein said control circuit generates [the] different key data [per logic sector on said storage medium when writing the data] for each writing to said unit storage areas.

14. (Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit has:

a write mode of encrypting the key data with a first [one] password, writing the encrypted key data to said storage medium, encrypting a second [other] password with said first [one] password, and writing said second [other] encrypted password; and

a read mode of decoding said second [other] encrypted password with said second [the other] password, obtaining said first [the one] password, and thereafter decoding the encrypted key data with said first [the one] password.

15. (Amended) A storage medium having protected data is stored with;

a plurality of key data encrypted with a different password for each of a plurality of unit storage areas of said storage medium [with a password]; and

data encrypted with the different key data for each said unit storage area of said storage medium.